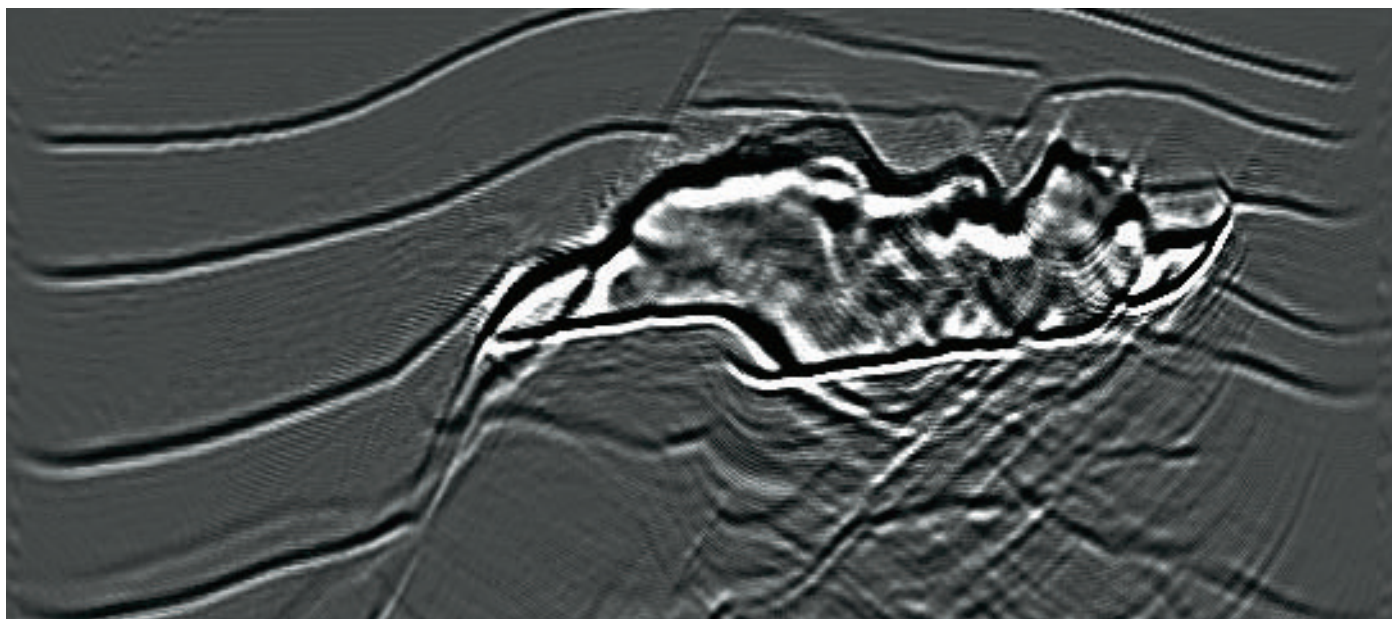


BITS

computing & communications news

APRIL 1997

COMPUTING, INFORMATION, AND COMMUNICATIONS (CIC) DIVISION • LOS ALAMOS NATIONAL LABORATORY



Scientists at LANL were involved in a multi-year collaborative project with U.S. oil companies to advance the technology of three-dimensional prestack depth migration. The cornerstone of the project was to develop an integrated software system that would image and analyze the structures beneath salt formations. The image shown above depicts a vertical slice of the Gulf of Mexico salt dome. This technology will lead to more effective development of significant additional oil and gas reserves. The project offers a unique opportunity to bring together the expertise at Los Alamos in computational modeling, algorithm development, and use of its advanced computer systems with the petroleum industry's access to seismic data and its experience and capability in seismic data processing and interpretation. The project is being funded by the Advanced Computational Technology Initiative Program. The LANL project leader is Mike Fehler, and the Advanced Computing Laboratory team leader is Eugene Gavrilov.

Inside this issue

Feature Articles

Video Teleconference Center Offers New Capabilities	1
Improved Access to Electronic Journals from Your Desktop	2
DOE Energy Database Now Available in a WWW Version	3

Microcomputing News

The REDI Project	4
The Universal Serial Bus (USB) Has Arrived	6

WWW at LANL

Web Security in the Open Network Security Model	7
--	---

In the Classroom

Research Library Training	13
Labwide Systems Training	14
Vendor Computer Training	16

Index	23
--------------	----

Customer Service Center(505) 665-4444 or cichelp@lanl.gov

Because of the wide variety of CIC computing services, numerous facilities are available to address your questions. If you are uncertain whom to call, you can always call the Customer Service Center (CSC). CSC consultants are trained to either answer your question or locate someone who can. To reach the appropriate consultant, dial 665-4444 and make your selection from the following choices:

Option 1: New user topics including e-mail, passwords, smartcards, registration, and World Wide Web.

Option 2: Labwide Systems such as Travel, Time and Effort, and Purchase Cards.

Option 3: Scientific computing, storage systems, and networking.

Option 4: Classroom instruction and training.

Option 5: Desktop Consulting for PC and Macintosh software and network configurations.

Consulting Via E-Mail

Customer Service Center.....cichelp@lanl.gov

Scientific and engineering computing.....consult@lanl.gov

Administrative and business computing.....labwide@lanl.gov

Passwords and registration.....validate@lanl.gov

Macintosh computing.....Mac-help@lanl.gov

PC computing.....PC-help@lanl.gov

UNIX computing.....UNIX-help@lanl.gov

Other Useful Numbers

Advanced Computing Laboratory.....665-4530

Central Computing Facility.....667-4584

Network Operations Center.....noc@lanl.gov or 667-7423

Telephone Services Center.....667-3400

Video Teleconference Center Offers New Capabilities

The Video Teleconference Center (VTC) has a new dial-up, ISDN-based Picturetel, Concord 4500 System. This new system greatly expands the number of sites available for teleconferences. Previously, we could access only those sites that were connected to specific networks, such as the DCTN and CSVN. With the Picturetel system, we can provide access to virtually any other teleconferencing facility worldwide. The Picturetel system provides site-to-site conferences as well as multiple-site conferences. The system is certified on FTS-2000/AT&T and Sprint bridges, and we have already used it for conferences with numerous sites around the U.S. as well as with sites in Japan.

The VTC also maintains direct links to over 80 sites within the DOE complex and more than 290 sites within the DOD Complex. Additional links can be established to domestic, corporate, and private rooms. The VTC has two rooms available for teleconferences.



Video Teleconference Center Team (L to R): Diana Tuggle (team leader), Dolores Roybal, and Elevation Salazar

VTC: Room 1

Location: TA-3, SM-132, Room 331

Seating Capacity: 12

Security: Available for classified and unclassified conferences

Networks: Defense Commercial Telecommunications Network (DCTN), Common Secure Video Network (CSVN), FTS-2000/Compressed Video Transmission Services (CVTS), and FTS-2000/Switched CVTS.

VTC: Room 2

Location: TA-3, SM-200, Room 108

Seating Capacity: 6

Security: Unclassified conferences only

Networks: FTS-2000/CVTS

The VTC offers excellent graphics capabilities including high-resolution graphics with real-time interaction and image manipulation; standard-resolution graphics for color transparencies, view graphs, and photographs; and multimedia capabilities that support flip charts, 35-mm slides, and video-tape recording.

The cost for a teleconference is \$325 per hour, regardless of how many sites are connected. For reservations, please call us at (505) 665-3000 or contact us by e-mail at djr@lanl.gov or vina@lanl.gov. You can also drop by our main facility (Room 1) and we will be glad to schedule your conferences.

*Dolores Roybal, djr@lanl.gov (505) 665-3000
Customer Service Group (CIC-6)*

Improved Access to Electronic Journals from Your Desktop

A new, improved version of the Electronic Journals Web page is now available from the Research Library's home page (<http://lib-www.lanl.gov>). This new version allows you to search for electronic journals by subject category. For example, by selecting physics from the list of Subject Categories (see figure below), you can view a listing of all the physics journals currently available—right from your desktop. This new version also allows you to search for a particular journal title, and it provides a description of each journal along with any passwords required for access.

The Research Library currently provides access to over 300 electronic journals. Direct links to these electronic journals are provided from the new Web version of our on-line catalog (<http://lib-www.lanl.gov/edata/catalog.htm>), as well as from the Electronic Journals Web page (<http://lib-www.lanl.gov/cgi-bin/ejrnlsrch.cgi>).

New journals are continually being added as they become available. Recent additions include on-line journals from the American Institute of Physics such as Applied Physics Letters, and many of the IEE Proceedings series. Through a special agreement between Academic Press and members of the New Mexico Library Alliance, we recently received free access to 40 new electronic journals. These journals are from diverse subject areas such as botany, archeology, and economics. Please send your comments and suggestions about electronic journals to ej@mantaray.lanl.gov.

Nancy Sprague, nsprague@lanl.gov, (505) 667-5809
Research Library (CIC-14)

Electronic Journals

This list includes the titles and holdings of electronic journals currently accessible to LANL researchers. If you're also looking for print journals, try our [journals](#) page or continue your search in the [online catalog](#).

Search journal titles:

[Search Tips](#)

Alphabetic Listing

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Subject Categories

Astronomy	Current News	Library & Information Science
Biology/Genetics	Earth & Environmental Sciences	Mathematics
Business	Engineering	Physics
Chemistry	Government	Science (General/Popular)
Computer Science	International Affairs	Standards & Regulations

Subject Categories for Electronic Journals

DOE Energy Database Now Available in a WWW Version

The DOE Energy Science and Technology Database is now available using the same WWW gateway offered for the Research Library's Online Catalog. To access the WWW DOE Energy database, go to the Research Library's home page (<http://lib-www.lanl.gov/>), select "Electronic Databases," and then select the WWW link under "DOE Energy Science and Technology Database." You have now started a session in the WWW gateway and can choose either "DOE Energy" or the "Online Catalog." You can also go back and forth between these two databases, marking items from both, all during a single session.

The WWW interface features point and click tools, search and browse capability, links to electronic documents, links to related records, and marking of records to display, print, or e-mail (see figure below).

DOE Energy is a multi-disciplinary database containing worldwide references to basic and applied scientific and technical research literature published from 1974 to the present. Focusing primarily on energy and related topics, this database contains over 3.5 million records (with abstracts), including reports, journal articles, conference papers, patents, theses, software, and books.

Kathy Varjabedian, kv@lanl.gov, (505) 667-3031
Research Library (CIC-14)

[Search](#) [Comments](#) [Show Marks](#) [Databases](#)
[Browse](#) [Help](#) [Exit](#)

LANL Research Library: DOE Energy

Search: Select an **index** and enter your **search term(s)**;
then press your Enter key or click on the *Search* button.
For different word endings use ? as a wildcard.

Index	Search Term(s)
Title	
<div style="display: inline-block; background-color: black; color: white; padding: 5px 15px; margin: 0 5px;">Submit</div> <div style="display: inline-block; background-color: black; color: white; padding: 5px 15px; margin: 0 5px;">Clear Search</div>	

Note: If you get a *500 System Error*, click on the *Back* button of your Web browser, click on the *Exit* button of the current page, then try to start a new session. Click on the *Help* button for information on other known problems.

LANL Research Library Web Gateway, Version 1.0

WWW Interface for DOE Energy Database

The REDI Project

The REDI (Remote Electronic Desktop Integration) project is helping the Lab remain productive and competitive by reducing the cost and increasing the efficiency of desktop software and services. REDI can be translated as follows:

Remote—networked computer equipment located any distance apart.

Electronic—computer services delivered over the network rather than by a technician who comes to each workstation or by shrink-wrap disks and documents.

Desktop—software and hardware for Laboratory networked personal computers.

Integration—desktop services coordinated throughout the Lab to provide

- electronic, one-stop desktop hardware/software purchasing,
- electronic software distribution and maintenance,
- automated hardware and software inventoring,
- application sharing on a local server,
- help-desk automation,
- just-in-time training, and
- remote-access troubleshooting.

Launched in October 1996, REDI is a 2-year CIC Division project that will focus resources on increasing employee productivity and reducing operating costs. Over 10% of the Laboratory's budget is associated with desktop computers. According to industry studies (Gartner Group) as well as Lab measurements, the total cost of ownership (TOC) for each desktop computer can reach \$8300 per year.

Table 1 illustrates how human labor creates over 70% of that cost. With well over 13,000 desktop systems in use, the Lab's TOC is over \$100 million per year.

The mission of REDI is to reduce Laboratory desktop computer acquisition, management, and support costs through increased efficiency and labor-saving technologies. The goal of this new effort is to reduce the current annual total cost of ownership by 20%.

The REDI Project is modeled after studies by the Gartner Group, an information-technology consulting firm contracted by the Lab. Initiatives fall into three user service areas: Provide, Manage, and Help (see Figure 1).

Provide. REDI is phasing in the following services and strategies.

Electronic Software Distribution (ESD), an existing Lab service, provides software installation from a remote server to desktop systems (<http://www-cic2.lanl.gov/redi/esdtests/esd-site.cgi>). Because nearly 50% of the desktop costs are generated by manual software installation and upgrades, electronic distribution is the cornerstone for cost-effective desktop computer management. The Laboratory ESD has already provided over 48,000 licenses since its inception in 1993, and a newly designed interface offers the following additional services:

- On-line purchases,
- License transfers/returns,
- Server-wide virus detection,
- Transaction security,
- An inventory of a receiving machine's capacity,
- An inventory for conflicts,
- User notifications and management reports, and
- Support for Information Architecture standards.

Volume procurement strategies obtain best-of-breed selections at prenegotiated, discounted prices, which reduce both software and administration costs. For example, in January 1997, the Lab signed a contract through CJ Enterprises to participate in the Microsoft SELECT program (<http://www-cic2.lanl.gov/redi/esdtests/select.html>), which reaps significant software discounts now available through ESD and CJ Enterprises.

Table 1. Total Cost of Ownership for a Desktop Computer

Source of cost	Cost
User (self maintenance, troubleshooting, downtime, etc.)	\$4570 (55%)
Support (institutional technical support and maintenance)	\$1410 (17%)
Administration (procurement, property mgmt., records, etc.)	\$1160 (14%)
Capital (hardware and software costs)	\$1160 (14%)
TOTAL	\$8300

Preconfigured Systems will deliver computers with all optional hardware, peripherals, and required and requested software installed.

Product Evaluation will provide testing for usability before offering the products Labwide.

Manage. Software management techniques will aid acquisition and support decisions and keep software versions current.

Revision Control, a service already under way, ensures that software remains up-to-date. Automatically or at the discretion of the end user, software will receive revisions through the network.

Hardware and Software Inventories conducted remotely will tally desktop resources to manage acquisitions, maintain interoperability, insure legality and regulatory compliance, and make informed decisions regarding future volume purchases and other expenditures.

Software metering electronically finds what applications are in use to make informed decisions about license purchasing and to justify support.

Help. The rapid resolution of problems will increase user productivity.

Help Desk Automation will provide the following services to more rapidly resolve user's problems.

- Greater accessibility,
- Problem tracking with customer problem submission and closing,
- Diagnostic technologies,
- Problem-resolution reporting and analysis,
- Problem status reporting, and
- A comprehensive knowledge database.

Just-in-Time Training (JITT) delivers on-demand, electronic help packages built into the applications, which decrease the need for classroom and informal peer-to-peer training. Because JITT is interactive, self-paced, and applied to an immediate workplace situation, retention is very high. Help packages will receive usability evaluation as part of product evaluations.

Remote Access will overcome lost work time and frustration by allowing support personnel to open user-authorized sessions on remote desktops to provide one-to-one instruction, run applications, perform diagnostics, and alter and exchange files.

Measurements. The REDI Project will collect measurements on all initiatives to determine technological effectiveness and customer satisfaction and to ensure management by fact. Measurement tools include service usage rates, customer surveys, site visits, and built-in electronic feedback mechanisms.

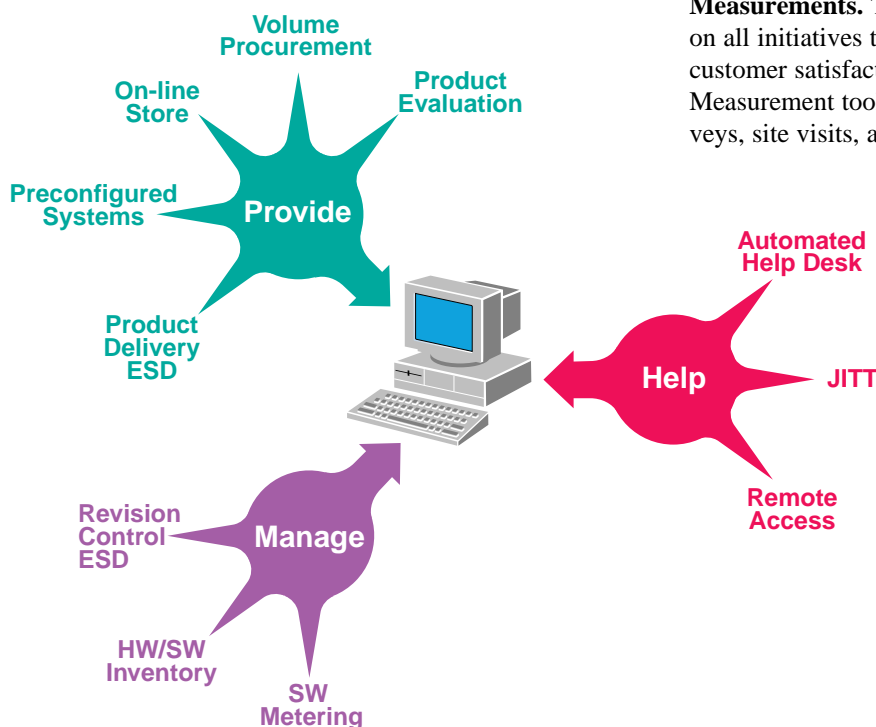


Figure 1. REDI Service Metrics

REDI commits to reducing the operational burdens on individual Lab organizations and providing users with the most efficient means of doing business, purchasing software and hardware, and receiving technical support.

For more information see the REDI proposal (<http://www-cic2.lanl.gov/redi/>) or contact the REDI project (redi@lanl.gov).

Marcia Hunsberger, (505) 665-4668
hunsberger_marcia@lanl.gov
 Communications Arts and Services
 (CIC-1)

The Universal Serial Bus (USB) Has Arrived



A new era of peripheral connectivity has arrived for the PC thanks to the Universal Serial Bus (USB). USB is a 12 megabits per second external bus that allows for a new level of flexibility and versatility. Input and output devices can be added to

your PC, even with the power on, and be configured and used immediately. Some examples of USB devices include mice, modems, keyboards, joysticks, telephones, tape drives, scanners, printers, digital audio devices, telephone PBX systems, and data gloves. The USB could replace your current serial ports, parallel port, mouse/keyboard ports, game/MIDI port, and monitor port. The USB connector is already showing up on the back of computers like AST, Compaq, Dell, Digital, Gateway 2000, HP, IBM, Sony, and Toshiba, and some USB devices are already on the market. It won't be long before those of us at LANL begin to take advantage of the USB technology on our desktops.

How It All Began

Since 1984, Apple Computer has had the ADB (Apple Desktop Bus) specification, which allowed for the effortless "plug-and-play" addition of mice, keyboards, display tablets, etc. On the PC side, however, your choices were pretty much limited to a mouse and a keyboard. To surpass this limitation, the leading PC manufacturers, Compaq, DEC, IBM, Intel, Microsoft, NEC, and Northern Telecom, got together and developed the specification for the USB. This specification was made available to the computer hardware industry, the results of which are only now coming to fruition.

What the Universal Serial Bus Offers

The USB allows for up to 127 devices to be connected to its bus. Each device automatically gets assigned an address when connected to the bus (no IRQs to set). The USB drivers work for both Windows 95 and Windows NT, and USB support was included in the recent OEM Windows 95 release (OSR 2.1). (There is currently no USB Macintosh version of the standard.) The USB allows for power management features on the bus and can provide up to .5 amps to its devices, eliminating the need for remote power cords and batteries. USB uses just four wires: two for data transfers and two for power.

The cabling uses a tiered-star topology with hubs to extend the number of connected devices. Future monitors will, in fact, have the option of a built-in USB hub. Finally, the new USB devices coming on the market will be cost-competitive with similar, current devices.

The USB standard supports what is called isochronous (or clocked) data transfers, which is needed for time-dependent data such as audio and video, as well as the more standard asynchronous data transfers used with such devices as mice and printers. USB is not intended for high-speed, prolonged data transfers, such as those required by hard drives. It can, for example, handle only up to a 4x or 6x CD ROM, and it cannot accommodate a write-able CD-ROM device. With the proper cable, you will be able to connect two PCs together for high-speed data transfers.

USB verses FireWire

The USB should not be confused with the new FireWire, IEEE 1394 standard. This is the new bus that Apple Computer invented for really high-speed (up to 400 megabits per second), prolonged data transfers. The two standards are set for different applications. USB will be used for mice, modems, and the like. Whereas, FireWire is intended for such things as digital camcorders, cameras, and super high-speed hard drives. We should start to see the major introduction of FireWire products in late 1997. It is expected that PCs in the future will have both USB and FireWire connection ports.

For More Information

Information about the USB can be found at www.usb.org. Here you can find its specification, an FAQ, and listings of available devices. Intel also has a good deal of information at <http://developer.intel.com:80/design/USB/>.

One of the things that surprised me most about the Universal Serial Bus is that it's already here. I had heard about it, but was recently surprised when setting up a new Dell computer to see the USB connector already installed, waiting for a device to be plugged in. The availability of USB devices should be forthcoming. It will be interesting to see what innovative uses will be found for this new standard.

*John Layne, jpl@lanl.gov, (505) 665-5090
Desktop Group (CIC-2)*

Web Security in the Open Network Security Model

In a Spring 1997 Nielsen survey, “lack of trust in the security of electronic payments” was identified as the main reason that people hesitate to make on-line purchases. Nothing too surprising about that. After all, who wants to trust their credit card number to the Web when the CIA’s own home page can be compromised?

In spite of the ongoing stories about break-ins, security bugs, viruses, etc., though, the Web has come a long way toward becoming more secure. We have encryption, filtering routers, single-use passwords, digital signatures, and more—a regular smorgasbord of treats for those of us who remember what it was like just a few years back.

The Information Architecture (IA) Project has recently adopted a series of standards that define a Laboratory Open Network Security Model. These standards address a variety of protocols (with more on the way) in the context of the Laboratory’s unclassified networks. Included are general standards for Web client and server security configurations, which seek to balance the need for openness in some areas (e.g., international collaborations) with the need for higher security in others (e.g., processing of sensitive information).

Throughout, the goal has been to make effective use of readily available tools to meet the real-world needs of the Laboratory community. These standards demonstrate how the Web has evolved into a mechanism that in many ways is arguably more secure than competing technologies.

The Nature of the Threats

The first step in evaluating a security model is to understand the basic nature of the threats it faces. These threats can be thought of in three broad categories: server threats, client threats, and network threats.

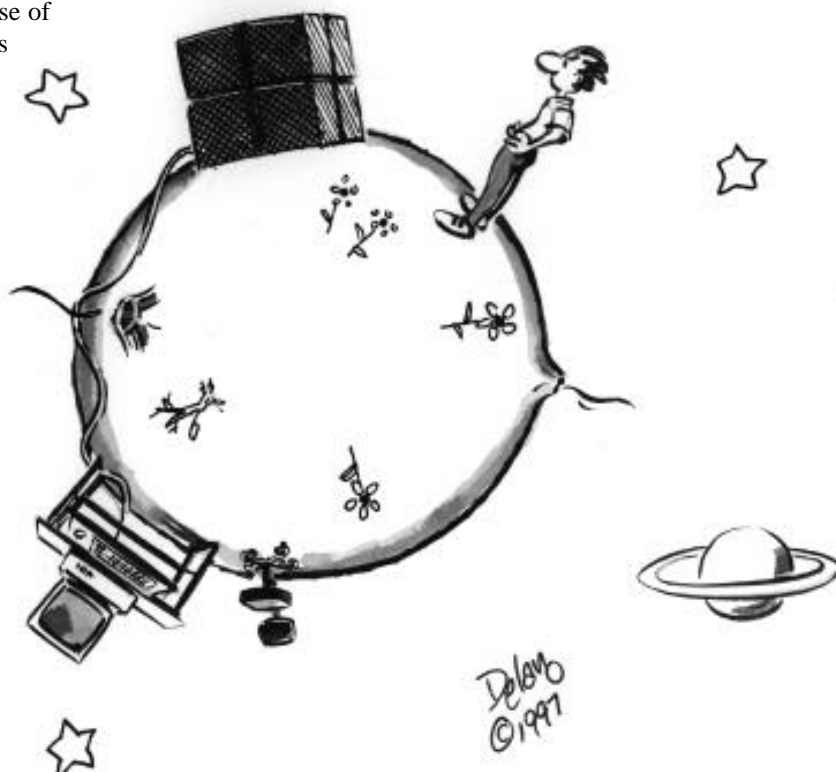
The basic threat to a Web server is that somebody will seek to use it in a way we don’t want them to. This is most commonly thought of as a prank break-in. For example, somebody gains log in access to a machine and replaces a “real” Web page with a mischievous substitute. This type of prank break-in is what happened to Web servers at NASA this March, the Air

Force last December, and the CIA last September. Aside from general embarrassment and the time needed to recover, little real harm usually comes from pranks such as these.

When somebody is able to gain log in access to the machine, however, there are a number of truly serious things that person could do. The most obvious is to gain access to sensitive information stored on the machine. Other possibilities include assuming the machine’s privileges to launch attacks on other machines, damaging files in non-obvious but destructive ways (it’s harder to fix something when you don’t realize anything’s happened), monitoring the machine’s network traffic to “sniff” passwords that are hidden from the outside, and so on.

Yet another class of server threat is the “denial of service” attack. This can come in a variety of forms (“half-open” TCP SYN floods, oversized ICMP datagrams, etc.), but the goal in each case is to use up the machine’s resources so it locks up and cannot serve others. Like the prank break-ins, denial of service attacks are generally more irritating than harmful,

though repeated attacks could easily become a significant problem.



Threats to a Web client can arise whenever we allow a program from somewhere else to execute on our desktop machine. The more permission we give the program, the greater the potential damage. Areas that have attracted attention include the following:

- A Web “cookie” is a piece of information the server stores on the client. Because nothing is executed and the server accesses no special information, the cookie isn’t a threat (at least not in any way that I’ve seen).

- A JavaScript script is able to execute a limited number of commands, but it cannot write to the client disk. It can potentially be used to trick users into revealing information they shouldn’t (such as passwords) or to use up machine resources until the machine locks up (another denial of service attack), but JavaScript can’t do permanent damage to the machine or its files.

- A Java program is able to execute a larger number of commands, and it can write to a restricted file space (i.e., “sandbox,” which varies in permissions depending upon the particular implementation of Java). A Java program can do everything JavaScript can plus cause damage within the sandbox, but it cannot cause any damage outside the sandbox. (The “Java bug” that made news in March 1996, though quickly corrected, was a vulnerability in certain implementations of the sandbox.)

- Other executables, such as ActiveX components and self-extracting downloads, have more freedom to operate within the desktop environment, which gives them a greater potential for causing damage. In order for a self-extracting software download to work, it needs access to the disk, which in turn enables malicious code to delete or replace files that might be critical to the operation of the machine. In serious cases, the only solution is to wipe the hard disk clean and reinstall the operating system.

Note: All of the above assessments are based on information I have seen as of the time of this writing. Although it is certain that additional specific vulnerabilities will be found, it does not seem likely that the general framework described above will change.

Network threats generally come through either the client or the server machine; once an attacker has compromised one of those machines, he/she can then use that machine as a basis for attacks on other machines.



Several examples were mentioned above as server threats. Similar attacks can come via the client. For example, an undetected ActiveX component could potentially hide in the background, act as a Trojan horse, and sniff the network traffic for users' passwords. Once the passwords were detected, they could be sent back out to the attacker, compromising users' accounts without their knowledge of the cause or source of the attack. I label these "network threats" because they are threats against the entire network, not just individual machines.

The Nature of the Needs

Taken in isolation, the nature of the threats might seem a good argument to just pull the plug between the internal network and the external world. After all, if there is no path through, then the network should be safe. (Even "should be" is not absolute, of course, because there are still threats like viruses carried on diskettes, stand-alone modems that can be attacked, etc.)

Before pulling the plug we need to remember that value is in fact added by allowing our open networks to connect to the external Internet. The word "internet" itself means "interconnected networks," and only by interconnecting our own networks are we able to take advantage of its capabilities. Electronic collaboration, information sharing, fact-based decision making, publishing, and more—all depend on some degree of openness in our networks.

In large part, our security needs are determined by the sensitivity of the information we are working with. In IA-6303: Internet/WWW Information Categories, the IA project identifies three broad categories of such information: public, internal, and sensitive. These are based on a variety of laws and other regulations that govern the Laboratory's operations, with the underlying details spelled out in IA-6304: Detailed Listing of Information Types.

Public information is "unlimited release" information intended for a global audience (such as BITS itself or the publicly released IA materials). To facilitate its dissemination, such information needs to be served as freely as possible, which in turn inevitably exposes us somewhat to potential threats. We can "wrap" the server against attacks via unneeded protocols, and we can keep up-to-date defenses against known threats. But as long as the Web continues to evolve as quickly as it is, the protection will always have potential vulnerabilities, and the machine itself will remain inherently at risk.

Internal information is the large class of information which is not ready or intended for public dissemination but which

would not cause serious problems if it were uncovered. Examples include drafts of articles that will eventually be publicly distributed, a broad range of meeting schedules and/or minutes, and similar unclassified, non-sensitive administrative information. Internal information warrants a certain level of protection (e.g., IP-address screening or HTTPd-level passwords), but it also generally warrants relatively free dissemination within the Laboratory community. The potential vulnerabilities to the server in this case primarily come from network threats (e.g., the risk that another machine sharing the network has been compromised).

In contrast, sensitive information is information that the Laboratory is bound by law to protect. Examples include medical, personnel, and security records (protected by the Privacy Act); protected Cooperative Research and Development Agreement (CRADA) information (protected by the terms of the CRADA); Unclassified Controlled Nuclear Information (UCNI, protected by the Atomic Energy Act); etc. For such sensitive information, we need to tightly restrict access. We'll want secure password authentication for users to demonstrate who they are, robust authorization to determine what information those users have permission to see, and encryption to prevent the data stream from being sniffed. Furthermore, because of the network threats outlined above, we'll want reasonable assurance that other machines sharing the server's network are themselves secure and not likely to be the source of attacks.

Client security is likewise driven in large part by the sensitivity of information being processed, both by the particular client and by the other machines on the network. Clients need to access information, but at the same time we'd like to provide some assurance, when we can, that they're not inadvertently accessing known threats.

The Basic Open Network Security Model

In IA-6C01: Laboratory Open Network Security Model (adopted February 3, 1997), the IA separates the Laboratory's Open Networks into two basic regions: (1) an Open Green region with minimal access restrictions, and (2) an Open Blue region with more controlled access and network-level security features (see Figure 1 on page 10).

In this illustration, the External Internet is the Internet at large, or everything outside the .lanl.gov name space. External collaborators generally reside in this area, as do employees on travel or change of station, and external information sources such as the IETF and CNN.

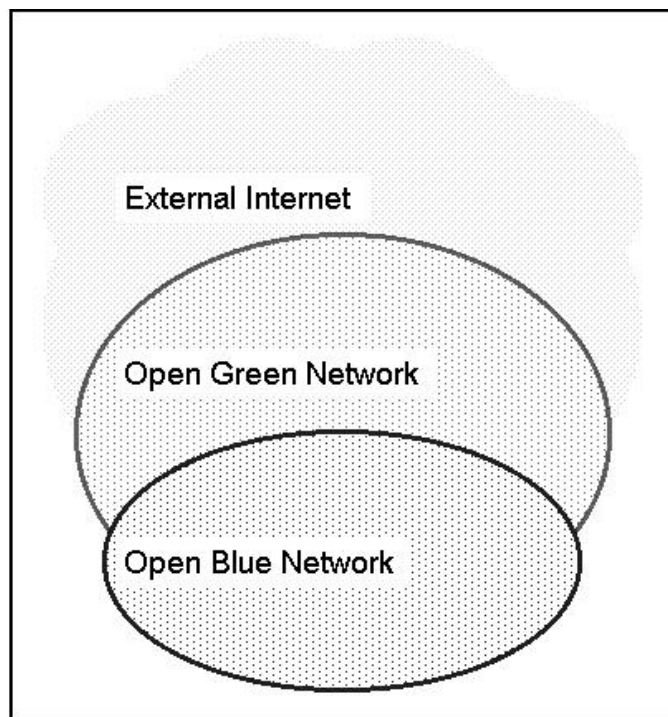


Figure 1: Open Network Security Model

The Laboratory's Open Green Network is separated from the External Internet by a Laboratory network gateway that imposes minimal restrictions. There are basic protections such as IP source-spoofing prevention, but the gateway does not act as a firewall that provides extensive protections. Traffic between the External Internet and Open Green Network is not controlled at the network level, though specific organizations may choose to add controls at the local level.

The Open Blue Network is separated from the External Internet and the Open Green Network by a distributed gateway consisting of routers, proxies, forwarders, and other tools. These protections are not adequate for classified computing, but they are considered adequate for protecting sensitive information.

The Open Blue is similar to the current Administrative Partition ("Admin"), with several basic distinctions:

- Protections placed on the Open Blue are developed through the IA process to allow input from a Laboratory-wide audience.
- Details of the Open Blue are openly published to facilitate awareness and to enable ongoing feedback and refinement.

- The Open Blue shares the same network backbone as the Open Green, unlike the Admin which requires a separate physical network partition. The shared backbone makes the Open Blue highly portable and leverages existing investments in the network infrastructure.

- Participation in the Open Blue is voluntary at the organization/subnet level, though adherence to its restrictions is mandatory for those who choose to participate.

- The Open Blue is a value-added service, intended to eventually serve a larger portion of the Laboratory than the current Admin.

Because participation in the Open Blue is voluntary instead of mandatory, its success depends on the value it offers to organizations—a deliberate competitive pressure intended to drive continual improvements in service.

Parts of the Open Blue are already implemented. By the time it is fully available, we anticipate that it will absorb the Admin and that other organizations will join as they see appropriate.

Web Server Security

Basic network-level Web server security for the Open Green and Open Blue is defined in IA-7101: Access to Laboratory Open WWW Servers (adopted March 6, 1997). This model encourages use of the Open Green network for public and internal information, and provides security in the Open Blue network to allow sensitive information to be served.

More specifically, the model does the following:

1. Places no restrictions on World Wide Web (WWW) communications to or from WWW servers in the Open Green region;
2. Places no restrictions on WWW communications between Open Blue clients and Open Blue servers; and
3. Requires the following limitations on WWW communications sent from the External or Open Green clients to the Open Blue servers: (a) communications are restricted to users with current ICN accounts, (b) communications must be encrypted, and (c) communications must pass through a transparent proxy (i.e., a machine that acts as a single gateway through which WWW communications with Open Blue servers pass).

In Figure 2, this model is illustrated with solid arrows representing unencrypted, unauthenticated traffic, and dashed arrows representing encrypted, ICN-authenticated traffic. Because the proxy is transparent, it is not included in this illustration.

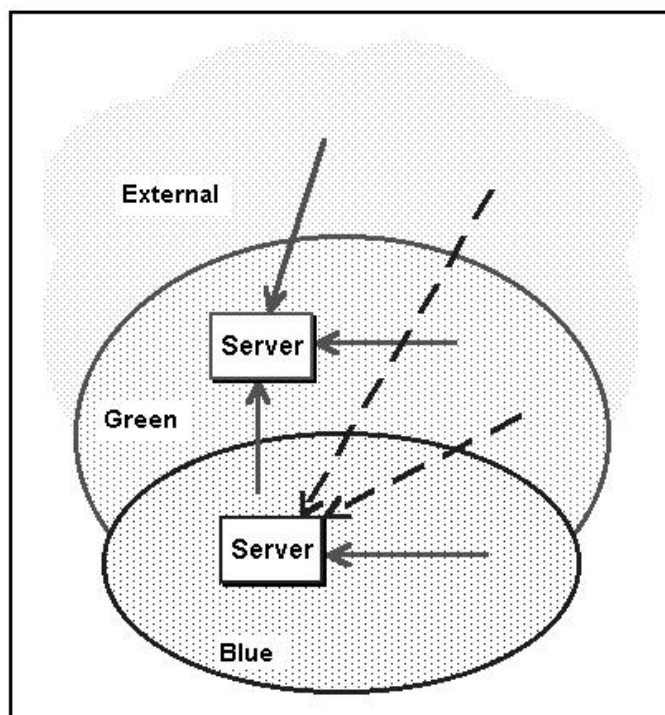


Figure 2: Access to Open WWW Servers

Encryption is most commonly done through the Secure Sockets Layer (SSL) protocol, which is widely deployed on modern browsers (including the IA standard Netscape 2.02+ and 3.0). SSL uses public key RSA encryption to transmit a private key, which is then used as the basis for a higher performance symmetrical encryption such as DES. (Although this issue has not yet been fully resolved, it seems likely that the IA will call for servers to be configured to require DES encryption, since DES has received DOE approval.)

This level of encryption allows users to use both multiple-use ICN passwords and single-use Secure ID smartcard passcodes. (Over the course of time the password/code mechanisms may evolve.) An upcoming IA RFC (anticipated for publication in April or May) describes a Central Web Authentication Service that Web administrators throughout the Laboratory can use to perform this authentication, thereby leveraging development work that has already been done.

The model illustrated in Figure 2 deals only with WWW access (i.e., HTTP via browsers). Other access to the servers (login, FTP, etc.) has other restrictions on it (e.g., encrypted ICN password or single-use passcode log ins for Open Blue servers).

It is important to remember that Web authors and developers do not need to reside on the same network as their servers. For example, I personally expect to have my desktop machine within the Open Blue network, due to the protections it provides, but plan to serve almost all of my Web space from an Open Green server to provide as much access to the information as possible. The overall network security model allows this to be easily done.

Web Client Security

Basic Web client security for the Open Networks is defined in IA-7201: Internet Access from Laboratory Open WWW Clients (approved March 27). In this model, security for Web clients (e.g., Netscape Navigator) is provided through a WWW Client Proxy that caches frequently accessed pages for improved user response time and controls access to sites known to be a risk due to identified viruses, malicious Java code, illegal activity, or other identified security risks.

As illustrated in Figure 3 on page 12, use of the WWW Client Proxy is

- required for Open Blue Clients accessing External sites,
- recommended but optional for Open Green Clients accessing External sites, and
- available but not required for connections that remain within the Laboratory Open Networks.

In order to foster the free sharing of information via the Web (and to avoid implications of censorship), access control is by exception rather than rule; that is, access is permitted to all sites except those which have been found to constitute security threats (as opposed to blocking access to all but approved sites). Attempts to access one of the controlled sites are redirected to a warning page which explains that access is blocked, why it is blocked, and who to contact if an exception is required.

This approach does not constitute an endorsement of sites that can be accessed through the Web Client Proxy or an assurance that all high-risk sites have been blocked. The only assurances are as follows:

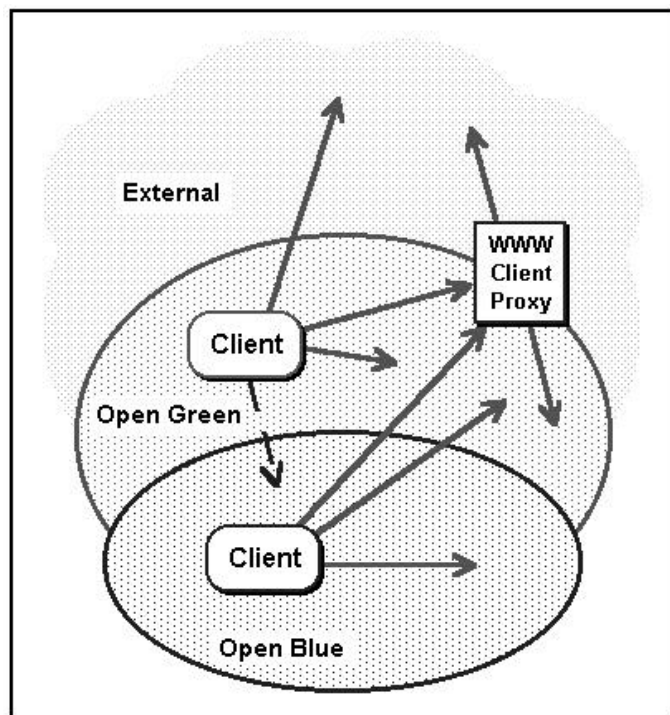


Figure 3: Access from Open WWW Clients

- some filtering is in place to reduce the overall danger,
- access logs are available to trace and correct problems that might occur (e.g., to help identify sources of problems), and
- a central mechanism is available for users to report high-risk sites they have encountered.

This model is based on the client proxy that has already been used by users in the Administrative Partition, so it has already been tested and refined.

Unlike the server security model which offers network-level protections only to Open Blue servers, the WWW Client Proxy is available for use throughout the Open Blue and Open Green networks. Individuals who want the additional security can freely configure their browsers to use the proxy, and/or organizations who want to protect their subnets at this level can require the proxy's use via their filtering routers without needing to subscribe to the rest of the Open Blue's requirements.

As a final note, the proxy itself is protected by restricting its use to Laboratory machines. We can freely share general information about the proxy's configuration with others, but the proxy remains subject to the official use restrictions placed on all government machines.

For More Information

For specific instructions on how to configure your browser to use the Web Client Proxy, please see IA-7201 or contact me at the address given below. (As of this writing, the machine address for the proxy is evolving, so whatever I write now is likely to be outdated by the time this article is published.)

For more information about the overall security model, please see IA-6C01 and its related standards at <http://www.lanl.gov/projects/ia/stds/>.

For more information about computer security in general, please see our Computer and Network Security activity area page at <http://www.lanl.gov/projects/ia-lanl/area/security/>.

For more information about IA work on Web issues, please see our General Internet/WWW activity area page at <http://www.lanl.gov/projects/ia-lanl/area/web/>.

Related topics of server security are discussed in the March 1996 BITS article "CGI Security." Other concerns related to client security are discussed in the July 1996 BITS article "Responsible Use of the Internet."

For more information about the IA Project in general and other work it has done, please see our home page at <http://www.lanl.gov/projects/ia/>.

For additional questions about the IA project or printed or e-mail copies of our materials, please feel free to contact me at the address given below.



Tad Lane, 505-667-0886, tad@lanl.gov
 Information Architecture Standards Editor
 Communications Arts and Services (CIC-1)

Research Library Training

The LANL Research Library provides training for using its specialized databases. Training sessions begin and end at times indicated below. Classes are free but you must preregister by calling the Research Desk at 7-5809 or sending e-mail to library@lanl.gov. Special classes and orientations can also be arranged.

Date	Time	Subject Matter
4/8/97	1:00 - 1:30 p.m.	Trial Access to Full-Text Business Literature
4/10/97	2:00 - 4:00 p.m.	InfoSurfing: Basic Web Searching Strategies
4/15/97	1:00 - 1:30 p.m.	Energy Database via the WWW
4/17/97	1:00 - 1:30 p.m.	Finding Business Information on the WWW
4/22/97	1:00 - 1:30 p.m.	Research Library Catalog via the WWW
4/23/97	11:00 - 11:30 a.m.	MELVYL (U of CA Specialized Databases)
4/23/97	1:00 - 1:30 p.m.	Finding Addresses and Phone Numbers on the WWW
4/29/97	1:00 - 1:30 p.m.	CASSI on CD
5/1/97	1:00 - 1:30 p.m.	Grant and Funding Information
5/6/97	1:00 - 1:30 p.m.	SciSearch at LANL—At Your Desktop!
5/8/97	1:00 - 1:30 p.m.	Finding Secret Information (Q-Clearance Required)

Labwide Systems Training

The Customer Service Group (CIC-6) offers training for users of Laboratory information systems. The CIC-6 courses offer training for a variety of personnel including property administrators, group secretaries, training coordinators, budget analysts, group leaders, or anyone needing to access training records, property records, costs, employee information, travel, chemical inventories, etc. Refer to the table below and on the following pages for specific information about courses currently offered.

Course Registration

You must have a valid ICN password before taking any of the courses shown in the table. To register for a course, call the CIC-6 Training, Development, and Coordination section at 667-9559 or access our Web page. From the LANL home page, look under "Services/Computing at LANL/Training" or enter the URL:

<http://www.lanl.gov:8010/computer-information/cic6/teampage.html>

Course Title	Date	Time	Cost	Course Number
Employee Development System - Basic Training (EDS I)	4/9/97	8:30-12:00	\$350	Course #5289
The course provides hands-on instruction to request course enrollment, use the on-line course catalog, retrieve training transcripts, and assign EDS authorities. The student will learn to create courses, add students to the courses, and generate several training reports.				
Employee Development System - Training Plans (EDS II)	4/23/97	1:30-5:00	\$350	Course #7155
Participants receive hands-on instruction to create and maintain training plans, assign assignment codes, and generate training plan reports. Attendees must have prior training in the Employee Development System (course #5289).				
Eudora Electronic Mail	TBA	1:30-3:30	\$175	Course #9762
This class is a hands-on class that teaches the participant how to use Eudora software to create, send, receive, and edit electronic mail messages. In addition to these procedures, the participant will learn what related settings mean and how to configure the system to meet his or her individual needs.				
Data Warehouse Basics	4/30/97	8:30-10:30	\$175	Course #11961
Students will receive hands-on training to generate standard reports and make quick queries from information in the data warehouse, a real-time collection of data tables from Laboratory financial, time-reporting, and personnel systems.				
Data Warehouse/ Financial Reporting	4/30/97	8:30-12:00	\$350	Course #11960
Students will receive hands-on training to generate standard financial reports and make on-line queries from information in the "data warehouse," a collection of data from Laboratory budgeting, accounting, and time-keeping systems.				
HTML Basics	4/22/97	8:30-12:00	\$350	Course #11605
Students will gain a basic understanding of HTML (Hypertext Markup Language), the language for the World Wide Web. Topics covered will be commands and standards, creating and editing documents, and authoring programs.				

Course Title	Date	Time	Cost	Course Number
HTML Tables	4/30/97	1:30–5:00	\$350	Course #11959
Students gain basic understanding of how to create various tables in HTML and new tags in HTML 3.0. Netscape-specific tags are also identified for clarity. Prerequisite: HTML Basics (Course #11605) or permission of the instructor.				
Introduction to the Internet: Beginning Netscape	4/29/97	8:30–10:30	\$175	Course #10961
Students gain basic understanding of the Internet and the World Wide Web and the use of Netscape as a browser to surf the Net. Topics covered are both Laboratory sites and open sites, along with practical uses of the Internet.				
Lotus Notes 4.0	4/10/97	8:30–12:00	\$350	Course #9917
This class provides hands-on instruction for Mac and PC users to use Lotus Notes software to create and send E-mail memos; fax documents; search databases; create filters, nicknames, banners, and doclinks; set defaults; and use multiple address books. In addition, participants learn how to use the memo, meetings, and discussion databases.				
Meeting Maker	4/8/97	1:30–4:00	\$175	Course #12395
Students learn how to create an address book, create personal groups, utilize the Auto-Pick feature, utilize e-mail integration with non-Meeting Maker users, and customize various Meeting Maker features.				
On-Line Forms	TBA	3:30–5:00	\$175	Course #9756
Participants will learn to use Netscape software to access Lab-wide information and forms. Using Jetform Filler software, participants will access, complete, and print forms such as the "ICN Validation Request," "Visitor Request for Unclassified Visits to Security Areas," and "Request for Quotation."				
Purchase Card System	TBA	1:30–2:30	\$175	Course #11924
Students will learn to reconcile monthly statement of account, submit reconciled statement of account for approval, print statement of account for audit records, and delegate reconciliation authority. Prerequisite: PCS Overview. Call Ruby O' Rear at 665-4523.				
Reporting with Infomaker	4/17–18/97	8:30–5:00	\$650	Course #11054
Hands-on training to query data and develop ad hoc, or non-standard, reports from the LANL data warehouse using Infomaker software.				
Time and Effort System (GUI)	TBA	8:30–10:00	\$175	Course #11018
The student will learn how to enter attendance, amend attendance, approve attendance, and submit exception and approval reports. Time codes and associated policies will be discussed. The student will also learn how to use the Information Manager utility to view and print reports.				
Travel	4/15/97	8:30–12:00	\$350	Course #12091
Hands-on training to submit and approve travel requests and expenses in the new Travel System which replaces the TRIPS on-line system and the post-travel expense worksheets.				

Vendor Computer Training

The Customer Service Group (CIC-6) supports vendor training in technical computing areas such as programming languages, system administration, networking, and World Wide Web development tools. The support provided by CIC-6 can be as limited as providing the appropriate facilities for a specific group or as extensive as coordinating training functions such as system administration, vendor acquisition, EDS administration, and class facilitation. The table below lists classes that are either currently being offered or are available on request. An expanded list of classes that are potentially available can be viewed on the Internet at

<http://www.lanl.gov:8010/computer-information/ComputerTraining/Vendor.html>

To request registration in any vendor course or for general assistance with vendor training, please contact the CIC-Division Vendor Training Coordinator at (505) 667-9399 or send e-mail to cic6-train@lanl.gov.

*Cost per student will vary depending on the total number of students enrolled in the class.

Course Title	Date	Time	Cost	Course Number
C Programming (Beginning)	Available on Request (5 days)		\$1600 – \$1900*	3996
Prerequisite(s): An understanding of and useful skills in a high-level programming language. A current ICN password is required. Topics Include: Introduction and Fundamentals; Basic Semantic Constructs - Getting; Base Level I/O With C; The Preprocess-Compilation Environment; Operators, Data Types, and Storage Classes; Control Flow Constructs; Conditional Constructs; Higher-Level Data Constructs in C; File I/O; UNIX Software Tools and POSIX System Calls.				
C Programming (Advanced)	Available on Request (5 days)		\$1600 – \$1900*	4777
Prerequisite(s): Useful skills and experience with the C Programming. A current ICN password is required. Topics Include: Data Structures, Algorithms, and OOP; An Advanced Clinic for C ; The ANSI C Recommendation X3.159; C and ANSI C War Stories; The Data Structure and the Assessment of Algorithms; Arrays; Structures; Unions; Stacks; Queues; Linked Lists; Recursive Functions; Binary Trees; Hashing; File Organizations Using the C Runtime Library; Standard Interprocess Communication Mechanisms; and An Introduction and Overview of AT&T's C++ 3.0.				
C++ for Experienced Programmers	6/23–27/97		\$1600 – \$1900*	9050
Prerequisite(s): Excellent C Language programming skills. Topics Include: Major Differences and Additions to ANSI C; Building C++ Classes; Introduction to Text I/O with C++; Function Overloading; Single Inheritance; Virtual Functions; Multiple Inheritance; Operator Overloading; Creating, Initializing and Assigning Objects; Passing and Returning Objects; Templates, Parameterized Functions and Classes; C++Stream I/O with the File System; and C++ Course Summary.				
Java Programming (Basic)	Available on Request (3 days)		\$800 – \$1,000*	11686
Prerequisite(s): Students must have the ability to create compiled programs using an advanced language (such as C or C++) and the knowledge to use basic Solaris commands and a World Wide Web browser (such as Mosaic or Netscape). Topics Include: Overview of the Java Programming Language, the HotJava WWW Browser, Applets, Audio and Animation, Importing Java Classes, Attaching Applets to HTML, Object-Oriented Programming Methodology, and Identification of Main Features of Java (including classes, servers, and security).				

Course Title	Date	Time	Cost	Course Number
Java Applications Programming	Available on Request (2 days)		\$600–\$800*	11687
Prerequisite(s): Completion of Beginning Java Programming course or equivalent knowledge. Topics Include: Developing Java Applications; Point-of-Sale Interfaces; Writing Java Code (demonstrating Java security, interactivity, graphics, audio, and animation); Java Class Packages and Subclasses; Memory Allocation and Garbage Collection Work; Interfaces, Exceptions, and Access Modifiers; Multithreading; and Extending Java.				
Java Programming Workshop	Available on Request (5 days)		\$1800–\$2100	12872
Prerequisite(s): Completion of Basic Java Programming and Java Applications Programming courses or equivalent knowledge. Topics Include: Designing and Developing Java GUI and Live Java Applications; Using a Subset of ANSI SQL to Communicate with a Relational Database; Programming a Java Network Connection and Interface; Understanding the Basic Structure of the JDBC-API; Constructing a Query-By-Example Interface, Including Data Parsing and Formatting; Listing Porting Issues Between Solaris 2.X and Windows NT; and Explaining the Steps for Including Native Methods in Java Code.				
Managing Internet Mail: Setting Up and Troubleshooting Sendmail and DNS	Available on Request (3 days)		\$1300–\$1800*	
Prerequisite(s): General knowledge of Unix system and network administration as well as experience with sending and receiving Internet electronic mail. Topics Include: Introduction to Using Electronic Mail; Theory of sendmail Operation; Understanding the sendmail.cf File; Address Rewriting Rules; Debugging sendmail; Understanding the Function of Sub-Domains in a Complex Mail Network; Setting Up Mail Sub-Domains and Mail Routing Hubs; Mail eXchanger (MX) Records and Mail Delivery in the Internet; Setting Up the Domain Naming System; Sendmail 8 - The Next Generation; Automatic Creation of sendmail.cf Files for Sendmail 8; and Verifying and Debugging sendmail.cf Files Generated by the sendmail Compiler.				
Perl Programming for the WWW	Available on Request (2–3 days)		\$500–\$700* per day	
Prerequisite(s): Programming skills with a light background in Perl and HTML. Topics Include: On-line Resources; Server Configuration; Permissions; Setuid Issues; Tainting; Safe Perl; Data Security; OO Programming; Web Modules; CGI Programs; CGI.pm; What Went Wrong?; CGI Template; Using Forms; Form Template; Input Widgets; Submit Widgets; Reset Widgets; Sample Form; Password Fields; Text areas; Hidden Fields; Checkboxes; Radio Boxes; Popup Menus; Listboxes; Image Maps; Random Links; libwww Modules; Sending Mail; Shopping Carts; Database Access; and Advanced Topics.				
SGI System Administration (Beginning)	Available on Request (5 days)		\$1800–\$2300*	11688
Prerequisite(s): Familiarity with using Silicon Graphics IRIS workstations and system administration procedures on other open system platforms. Topics Include: The Role of the System Administrator; Set Up and Configuration of an IRIS Workstation or Server; Supporting a Group of Silicon Graphics Users; System Security Maintenance; Backups and Recoveries; Configuration of Disk Drives; System Installation and Application Software; Attaching Terminals and Printers; Modifying the system Start Up and Shut Down Sequences; Automating Administrative Procedures; and Performing Basic System Troubleshooting.				
SGI Network Administration	Available on Request (5 days)		\$1800–\$2300*	11690
Prerequisite(s): Completion of Silicon Graphics System Administration (Beginning) course or equivalent knowledge and experience. Topics Include: Networking Fundamentals; Network Configuration; Network Troubleshooting; Resource Management with Network; Information Services; Domain Management with Domain Name System; Electronic Mail with Sendmail; Remote File Sharing with Network File System & Automounter; Network Performance Monitoring; and Network Security.				

Course Title	Date	Time	Cost	Course Number
SGI System Administration (Advanced)	Available on Request (5 days)		\$1800–\$2300*	11689
	Prerequisite(s): Completion of Silicon Graphics System Administration (Beginning) course or equivalent knowledge and experience. Topics Include: System Error Monitoring; Kernel Reconfiguration and Debugging; System Monitoring Tools; Process Management; MultiProcessor CPU Management; Memory Management and Tuning; Swap Management and Tuning; Disk Management and Tuning; XPS Filesystem Management; and System Security Concepts.			
Solaris 2.X System Administration (Beginning)	Available on Request (5 days)		\$1600–\$2000*	7477
	Prerequisite(s): Knowledge of Unix commands and an editor. Topics include: Custom installation of Solaris2.X server; Add peripheral devices; Use format utility to display partition information; Compress and send binary files; Change system run levels; Add startup files for additional services; Add and remove software packages; Configure terminals and modems; Administer disks and file systems; Discuss basic networking concepts; Configure NFS to support the client-server environment; Use the automounter; Add and remove diskless clients; Back up and restore file systems; Perform basic recovery and troubleshooting procedures; Configure and administer the NIS+ environment.			
Solaris 2.X Network Administration	Available on Request (5 days)		\$1600–\$2000*	8107
	Prerequisite(s): Completion of Solaris 2.X System Administration (Beginning) class or equivalent knowledge and experience. Topics Include: Network Configuration; Remote Installation Procedures; Advanced Security Techniques; Troubleshooting Techniques; Customizing Sendmail; Network Application Tools; and Name Service Configuration.			
Sybase SQL Server Administration	Available on Request (5 days)		\$1800–\$2100*	12913
	Prerequisite(s): Prior experience with SQL and familiarity with SQL servers and databases. Topics Include: SQL Server Environments and Installation; Resource Allocation and Management; Creating Databases; Modifying Default SQL Server Configuration; Backing Up Databases and Transaction Logs; User Permissions; Monitoring and Troubleshooting; Connectivity Issues; and Auditing.			
Sybase Performance Design and Tuning	Available on Request (5 days)		\$1800–\$2100*	12914
	Prerequisite(s): Sybase SQL Server Administration or equivalent knowledge and experience. Topics Include: Tuning Transact SQL Queries; Optimizing Locking at the Application Level; Tuning Transaction Processing; Working with Cursors; Benchmarking Techniques; and Optimizing Hardware Device Usage.			
UNIX (Basic)	Available on Request (4 days)	8:15–12:00	\$400	
	Prerequisites: Basic computer literacy (knowledge of the keyboard and mouse) are helpful. Topics: Getting Started; UNIX File System; Editing with VI; Manipulating Files; Using C-Shell Features; Customizing Your Environment; Navigating the Network; Job Control; Generic UNIX E-mail; and Electronic Mail Registration (EMR).			
UNIX (Advanced)	Available on Request (4 days)	8:15–12:00	\$400	
	Prerequisites: The Basic Unix class or equivalent knowledge. Topics: File Manipulation; File Reorganization; Network File System Concepts; Introduction to C-Shell Scripts; Conditional Execution; Shell Programming; The Korn Shell; Korn Shell Script Features; and SED Filtering Tool.			

INTEGRATED COMPUTING NETWORK (ICN) VALIDATION REQUEST

Instructions:

- (1) Complete all parts of this form that apply to you. Please take note of the "Special Requirements" section and complete any applicable parts.
- (2) Manager (Group Leader or above) authorization and signature are required for all validation requests.
- (3) Before submitting this request, ensure that your Employee Information System (EIS) information is current.
- (4) Once completed, either mail this request to the Password Office at MS-B251, fax it to (505) 667-9617, or, if you are cleared, handcarry it to TA-3, SM-200, Room 257.

If you have questions call (505) 665-1805 or send e-mail to validate@lanl.gov

Owner Information

Z-Number (if you have one)		Name (last, first, middle initial)	
LANL Group	Phone Number	LANL Mail Stop	Citizenship (Foreign National see "Special Requirements-Foreign National")

Check LANL affiliation:
☐ LANL employee
☐ Contractor _____
(specify contract company)
☐ External user _____
(specify employer)
☐ Other (specify) _____

Send password / smartcard to:
☐ Mail Stop or ☐ Mail to address indicated below

Name / Organization

Address

City, State, Zip Code

Access Check access method and needed partitions:

Access method:	<input type="checkbox"/> ICN Password	<input type="checkbox"/> Smartcard	<input type="checkbox"/> Both
<input type="checkbox"/> Open partition (e.g., open machines, or for dial up access)			
<input type="checkbox"/> Administrative partition (e.g., Travel, Data Warehouse, IA [BUCS, Stores], IB [EIS, FMIS, PAIRS]) If you are not a cleared LANL employee, see required steps in section "Special Requirements-Administrative Partition".			
<input type="checkbox"/> Secure partition (i.e., secure machines) A Q-clearance is required for secure access. After obtaining Manager signature for Secure access, handcarry this form to the Password Office to obtain your Secure account.		<div>I certify this person does require secure access: _____ Manager Signature (Group Leader or above) Date</div>	

Password Office Use Only

New <input type="checkbox"/>	Change <input type="checkbox"/>	Clearance Status	Processed	Lv	Smartcard Serial #
Comments: _____ _____					

Special Requirements

Administrative Partition

Lab-Wide Systems (e.g., Travel, Data Warehouse, IA [BUCS, Stores], IB [EIS, FMIS, PAIRS])

☐ Under 18 years of age If you need to access Administrative systems, your Group Leader must provide a memo accepting responsibility for your actions and justifying your need for access. This memo is to accompany all forms taken to the security briefing (see "Contractor or Non-Cleared") section below. You may not access the Secure Partition.

☐ Contractor or Non-Cleared Phone (505) 665-4444 (option #2) to obtain Access Authorization packet.
Phone (505) 667-9153 to schedule a security briefing.
Bring all forms including this ICN Validation Request to the security briefing for approval.

CIC-6 Security Briefing Approval Signature

Date

☐ Foreign National

Attach a copy of Form 982 (REQUEST FOR UNCLASSIFIED VISIT OR ASSIGNMENT BY A FOREIGN NATIONAL) with all approval signatures. Be sure Box #11 of Form 982 is completed. If you are not a visitor/assignee under a LANL/DOE approved Visit / Assignment Request, attach written justification from your host Group Leader or Division Director describing your need to access the ICN.

Authorization (required)

Print Manager Name (Group Leader or above)	Manager Z-Number	Group
Manager Signature (Group Leader or above)	Mail Stop	Date

If you are NOT a LANL employee, obtain your LANL contact's signature in addition to the contact's manager's signature.

NOTE: LANL contacts are regular Laboratory employees. Contacts are responsible for obtaining annual re-authorizations, forwarding renewal notices, and notifying the ICN Password Office of changes in user or contact status.

Print LANL Contact Name	Contact Z-Number	Phone Number	Group
LANL Contact Signature	Mail Stop	Date	

NOTE: All Laboratory computers, computing systems, and their associated communication systems are for official business only. By completing this validation request and signing for a password and/or smartcard, you agree not to misuse the ICN. The Laboratory has the responsibility and authority to periodically audit user files.

Reader Feedback

Feedback helps us to provide a document that responds to the changing needs of its readership. If you have comments or questions about this publication, please let us hear from you. We have reserved the back of this form for that purpose. We also accept articles for publication that are of interest to our readers. Contact the managing editor for more information. This form is also used for new subscriptions, deletions, or changes. Instructions are on the back. If you prefer to contact us by E-mail, send your comments and/or subscription request to finney@lanl.gov.

Do Not Staple
Fold on This Line First



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 88 LOS ALAMOS NM

POSTAGE WILL BE PAID BY THE ADDRESSEE

MAIL STOP B251
ATTN: MIKE FINNEY, MANAGING EDITOR
CUSTOMER SERVICE GROUP (CIC-6)
LOS ALAMOS NATIONAL LABORATORY
PO BOX 1663
LOS ALAMOS NM 87544-9916



Do Not Staple, Seal with Tape
Fold Here

cut along dashed line

This image shows a single sheet of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page. There are approximately 20 lines visible. The paper has a slight shadow on the right side, suggesting it's resting on a surface. There is no handwriting or other markings on the paper.

BITS is published by Los Alamos National Laboratory. If you would like to be added to or deleted from our mailing list, please check the appropriate line, complete the form below, and mail us the form.

_____ Delete my name from the BITS mailing list.

_____ Change my name/address as indicated below.

Date

Mail Stop

Organization

State

Zip

Number of copies

Employee Z#

INDEX

Keywords	Title of BITS Article	Date	Page
<i>Apple</i>	<i>Apple's NeXT OS Plans</i>	<i>Feb. '97</i>	<i>17</i>
<i>ASCI</i>	<i>The Accelerated Strategic Computing Initiative (ASCI)</i>	<i>Feb. '97</i>	<i>1</i>
<i>Advanced Networking Projects</i>	<i>Advanced Networking Projects Support High-Performance Computing at Los Alamos</i>	<i>Nov. '96</i>	<i>2</i>
<i>Beta</i>	<i>The Phasing out of Beta and Its Alternatives</i>	<i>Nov. '96</i>	<i>8</i>
<i>BITS</i>	<i>Announcing a Special Edition of BITS: Introduction to Computing at Los Alamos</i>	<i>May '96</i>	<i>1</i>
	<i>Special Edition of BITS Available On-Line</i>	<i>July '96</i>	<i>10</i>
<i>Challenge</i>	<i>Challenge to Start Seventh Year</i>	<i>Sept. '96</i>	<i>4</i>
<i>CIC (Computing, Information, & Communications)</i>	<i>New CIC Annual Report Available On-Line</i>	<i>July '96</i>	<i>10</i>
	<i>CIC Implements New Recharge Processing System</i>	<i>Sept. '96</i>	<i>1</i>
<i>CIC-4</i>	<i>CIC-4 Awards External Paging Contract and Expands Local Paging Capabilities</i>	<i>Aug. '96</i>	<i>5</i>
<i>CIC-6</i>	<i>The CIC-6 Vendor Training Program</i>	<i>Apr. '96</i>	<i>5</i>
	<i>Desktop Consulting Moves to CIC-6</i>	<i>Feb. '97</i>	<i>6</i>
	<i>CIC-6 Provides Desktop Consulting</i>	<i>Mar. '97</i>	<i>1</i>
<i>CIC-17</i>	<i>CIC-17 Offers Highlight Color Printing</i>	<i>Apr. '96</i>	<i>12</i>
<i>Cluster</i>	<i>Cluster Tutorials on the Web</i>	<i>Aug. '96</i>	<i>8</i>
	<i>Maple on the Cluster</i>	<i>Aug. '96</i>	<i>11</i>
	<i>TeX on the Cluster</i>	<i>Nov. '96</i>	<i>13</i>
	<i>IBM XL High-Performance Fortran Now Available on the Open Cluster</i>	<i>Nov. '96</i>	<i>14</i>
<i>Cray</i>	<i>Cray CF90 Programming Environment 2.0 for PVP and SPARC Systems</i>	<i>Apr. '96</i>	<i>6</i>
	<i>Cray Programming Environment 2.0 Tools</i>	<i>May '96</i>	<i>2</i>
	<i>The New Opportunity Scheduler for Crays</i>	<i>May '96</i>	<i>8</i>
<i>Database</i>	<i>NTIS Research Database at Your Desktop</i>	<i>July '96</i>	<i>4</i>
	<i>DOE Energy Science & Technology Database Coverage Expanded</i>	<i>Feb. '97</i>	<i>7</i>
	<i>BIOSIS Database Now Available Via CIC-14</i>	<i>Feb. '97</i>	<i>7</i>
<i>Desktop</i>	<i>Laboratory Desktop Software Standards</i>	<i>Apr. '96</i>	<i>1</i>
<i>E-mail Attachments</i>	<i>How to Get Unattached to E-mail Attachments Part 1: A Look at the Macintosh</i>	<i>May '96</i>	<i>10</i>
	<i>How to Get Unattached to E-mail Attachments Part 2: A Look at the PC</i>	<i>June '96</i>	<i>8</i>
	<i>Don't Get too Attached to Your [E-mail] Attachments</i>	<i>Oct. '96</i>	<i>8</i>
	<i>Capturing E-mail as a Record at LANL</i>	<i>Nov. '96</i>	<i>5</i>
<i>Enterprise Information Systems</i>	<i>Enterprise Information Systems</i>	<i>Oct. '96</i>	<i>6</i>
<i>External Computing Project</i>	<i>External Computing Project</i>	<i>Dec. '96</i>	<i>9</i>
<i>GNU Utilities</i>	<i>GNU Utilities Now Available Locally on /usr/lanl</i>	<i>Dec. '96</i>	<i>10</i>
<i>HPD (Heterogeneous Parallel Debugger)</i>	<i>HPD: Heterogeneous Parallel Debugger</i>	<i>Nov. '96</i>	<i>2</i>
<i>HTML (HyperText Markup Language)</i>	<i>The Current State of HTML</i>	<i>Dec. '96</i>	<i>11</i>
	<i>The Current State of HTML: Part II</i>	<i>Feb. '97</i>	<i>8</i>
<i>ICN (Integrated Computing Network)</i>	<i>ICN Host Status Now Available on the Web</i>	<i>Apr. '96</i>	<i>17</i>
	<i>Questions and Answers from the ICN Consulting Office</i>	<i>June '96</i>	<i>2</i>
	<i>ICN Password Office Provides FAQ Web Page</i>	<i>Oct. '96</i>	<i>7</i>
	<i>The ICN Consulting Office</i>	<i>Feb. '97</i>	<i>4</i>
<i>Internet</i>	<i>Responsible Use of the Internet</i>	<i>July '96</i>	<i>1</i>
<i>ISDN (Integrated Services Digital Network)</i>	<i>Orders for ISDN Suspended</i>	<i>July '96</i>	<i>4</i>
<i>JavaScript</i>	<i>JavaScript Observations and Tips: Part I</i>	<i>Mar. '97</i>	<i>10</i>
<i>Lab-Wide Systems</i>	<i>Questions and Answers for Lab-Wide Systems Users</i>	<i>Apr. '96</i>	<i>14</i>
	<i>Consulting for Lab-Wide Systems</i>	<i>Dec. '96</i>	<i>1</i>
	<i>Lab-Wide Information Systems Descriptions</i>	<i>Dec. '96</i>	<i>3</i>

Keywords	Title of BITS Article	Date	Page
<i>Lab-Wide Systems</i>	<i>Authorities for Lab-Wide Systems</i>	<i>Dec. '96</i>	<i>6</i>
	<i>Common Validation Error Messages and Possible Solutions for Lab-Wide Systems</i>	<i>Feb. '97</i>	<i>11</i>
	<i>Accessing GUI Lab-Wide Systems on the Macintosh</i>	<i>Mar. '97</i>	<i>9</i>
<i>LSF (Load Share Facility)</i>	<i>Life in the Fast Lane: Using LSF to Cut Down on Cluster Computing Time</i>	<i>June '96</i>	<i>3</i>
<i>Macintosh</i>	<i>Four Macintosh Shareware Programs That Will Make Scientists Happy</i>	<i>Sept. '96</i>	<i>9</i>
<i>Maple</i>	<i>Vendor Training Available for Maple Users</i>	<i>Dec. '96</i>	<i>17</i>
<i>Mathematica</i>	<i>Mathematica Tutorial Available on the Web</i>	<i>Feb. '97</i>	<i>12</i>
<i>Medicare</i>	<i>Computer Sleuths Hunt for Medicare Bandits</i>	<i>Sept. '96</i>	<i>2</i>
<i>Mercury</i>	<i>Mercury Open-Secure ICN File Transfer Service Now Available</i>	<i>Oct. '96</i>	<i>4</i>
	<i>Workout with Mercury—Step by Step File Transfer Using Mercury</i>	<i>Dec. '96</i>	<i>14</i>
<i>Microsoft SELECT</i>	<i>Software Discounts Available through Microsoft SELECT</i>	<i>Feb. '97</i>	<i>6</i>
	<i>New Microsoft SELECT Program Lowers Software Costs</i>	<i>Mar. '97</i>	<i>2</i>
<i>Modeling</i>	<i>Modeling Ultra-Low Loss Accelerators</i>	<i>Nov. '96</i>	<i>1</i>
<i>MPI (Message Passing Interface)</i>	<i>Getting the Most out of MPI</i>	<i>July '96</i>	<i>5</i>
<i>MIME (Multipurpose Internet Mail Extensions)</i>	<i>A Closer Look at MIME</i>	<i>July '96</i>	<i>11</i>
<i>Network</i>	<i>Statistics on Network and Telephone Services at LANL</i>	<i>May '96</i>	<i>4</i>
<i>OAG (On-line Airline Guide)</i>	<i>OAG Service Announcement</i>	<i>Sept. '96</i>	<i>5</i>
<i>PAGES (Print And Graphics Express Station)</i>	<i>PAGES Hardware Status Now Available on the Web</i>	<i>Apr. '96</i>	<i>13</i>
	<i>PAGES Replaces ILFORD Printer with FUJI Printer</i>	<i>Nov. '96</i>	<i>9</i>
<i>Password</i>	<i>On-Line Semiannual Passwords for Secure Users</i>	<i>Apr. '96</i>	<i>5</i>
<i>PVM (Parallel Virtual Machine)</i>	<i>PVM: Easier to Use</i>	<i>Apr. '96</i>	<i>8</i>
<i>Research Library</i>	<i>Research Library's Monthly Electronic Newsletter</i>	<i>Aug. '96</i>	<i>8</i>
	<i>Research Library's WWW Online Catalog</i>	<i>Mar. '97</i>	<i>4</i>
<i>SciSearch</i>	<i>New Weekly Alerting Service via SciSearch at LANL</i>	<i>Nov. '96</i>	<i>6</i>
<i>Secure Unclassified</i>	<i>Good-Bye Secure Unclassified</i>	<i>Oct. '96</i>	<i>5</i>
<i>Telephone Services</i>	<i>FTS 2000 Provides Savings for LANL Telephone Services</i>	<i>Aug. '96</i>	<i>6</i>
<i>Telnet</i>	<i>Configuring Telnet as a Supporting Application under Netscape 3.X</i>	<i>Mar. '97</i>	<i>7</i>
<i>World Wide Web (WWW or Web)</i>	<i>Creating Effective Web Page Backgrounds</i>	<i>Apr. '96</i>	<i>15</i>
	<i>Mathematical Reviews Available On-line through the Research Library Web Page</i>	<i>May '96</i>	<i>3</i>
	<i>Copyright and the World Wide Web</i>	<i>May '96</i>	<i>5</i>
	<i>CIC-1 Web Team Designs and Revises Web Pages</i>	<i>June '96</i>	<i>1</i>
	<i>Barnstorming the Web</i>	<i>June '96</i>	<i>5</i>
	<i>Images on the Web: Some Tips</i>	<i>Aug. '96</i>	<i>1</i>
	<i>Finding Phone Numbers and Addresses via the Web</i>	<i>Sept. '96</i>	<i>5</i>
	<i>Images on the Web: More Tips</i>	<i>Sept. '96</i>	<i>6</i>
	<i>Mariachis Weave Beethoven? More Tips and Tricks [on the Web]</i>	<i>Oct. '96</i>	<i>1</i>
	<i>Getting a Web Site Indexed</i>	<i>Nov. '96</i>	<i>10</i>
	<i>Tools for Developing Web Pages in the Windows Environment</i>	<i>Dec. '96</i>	<i>18</i>
<i>Windows 95</i>	<i>Windows 95 SLIP/PPP Installation</i>	<i>Apr. '96</i>	<i>18</i>
	<i>Keyboard Shortcuts for Windows 95</i>	<i>Dec. '96</i>	<i>22</i>
	<i>Windows 95 SLIP Support Installation</i>	<i>Feb. '97</i>	<i>13</i>

Produced by the Computing, Information, and Communications (CIC) Division

Managing Editor: Mike Finney (667-2241 or finney@lanl.gov)

Design: Gloria Sharp and Mike Finney

Illustration: Dave Delano

Printing: Media Group (CIC-17)

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.

All company names, logos, and products mentioned herein are trademarks of their respective companies. Reference to any specific company or product is not to be construed as an endorsement of said company or product by The Regents of the University of California, the United States Government, the U.S. Department of Energy, nor any of their employees. The Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; therefore, the Laboratory as an institution does not endorse the viewpoint of a publication or guarantee its technical correctness.

Los Alamos
NATIONAL LABORATORY

Los Alamos

NATIONAL LABORATORY

Los Alamos, New Mexico 87545

BITS is published monthly to highlight recent computing and communications activities within the Laboratory.

We welcome your suggestions and contributions.

BITS can be accessed electronically via Web browsers such as Mosaic and Netscape. Enter the following URL:

<http://www.lanl.gov/Internal/divisions/cic/publications.html>

LALP-97-8 (3-97)

Nonprofit
organization
US Postage

PAID

Los Alamos, NM
Permit No. 107